CLAIM AMENDMENTS

32. (currently amended) A method for marking digital data ~~such that~~ to prevent the data ~~may be protected~~ from being copied or transmitted ~~unauthorized copying or transmission~~ without authorization, the method comprising the steps of:

~~(a) obtaining the digital data;~~

~~(b)~~ selecting a global copyright mask M;

~~(c) generating a content override mask X;~~

~~(d)~~ generating an authenticator Y;

generating a content override mask X ~~such that Y is~~ derived from ~~X~~ Y using a one-way cryptographic function;

~~(e)~~ selecting a data mask S to be a combination of X and M; ~~and~~

~~(f)~~ using the data mask S to create marked data from the digital data; and

transferring the marked data and Y to an entity configured to prevent copying or transmitting the marked data when the result of performing the one-way cryptographic function on Y is not detected in the marked data.

33. (currently amended) The method of claim 32 wherein the marked data includes additional embedded protection fields describing ~~one or more action that are~~ at least one action authorized by the data mask S.

34. (previously presented) The method of claim 32 wherein the marked data is compressed data.

35. (previously presented) The method of claim 32 wherein the marked data is in encrypted form.

36. (canceled)

37. (new) The method of claim 32 wherein the marked data is allowed to be copied or transmitted when M is not found within the marked data.

38. (new) The method of claim 32 wherein:

C15

a first party performs the steps of selecting M, generating Y, generating X, and selecting S; and

the first party sends the marked data to a second party by supplying Y to a sending device associated with said first party.

39. (new) The method of claim 38 wherein:

the first party sends Y to the second party;

the second party feeds Y to a writing device associated with the second party, enabling the marked data to be copied or transmitted by the second party once only; and

the writing device inhibits further propagation of Y, thereby preventing the marked data from being copied or transmitted more than once.

40. (new) The method of claim 32 wherein the marked data includes executable program code.

41. (new) A method for determining whether a requested action is authorized to be performed on some digital content, said method comprising the steps of:

applying a non-collision-resistant compression function to a plurality of portions of said digital content;

applying a one-way cryptographic function to an authenticator value;

determining whether the result of applying said one-way function is represented in results of said applications of said compression function; and

when said determining step finds that the result of applying said one-way function is so represented, allowing said requested action to be performed.

42. (new) The method of claim 41 wherein said requested action includes making a copy of said digital content.